(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 41 19 924 A 1**

(51) Int. Cl.[5]:
G 06 F 15/30
G 06 K 19/00
G 06 F 12/14

(21) Aktenzeichen: P 41 19 924.3
(22) Anmeldetag: 17. 6. 91
(43) Offenlegungstag: 24. 12. 92

DE 41 19 924 A 1

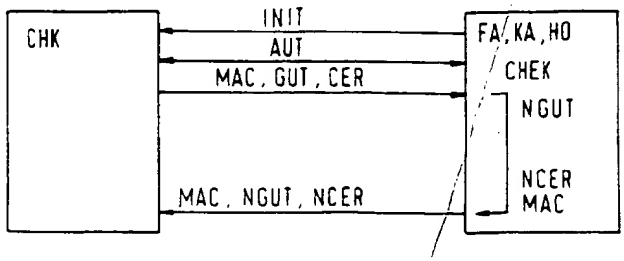
(71) Anmelder:
Siemens AG, 8000 München, DE

(72) Erfinder:
Hueske, Thomas, Dipl.-Math.; Pfau, Axel, Dipl.-Math., 8000 München, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Sicherung von ladbaren Guthaben in Chipkarten

(57) Die Chipkarte (CHK) wird für Debit-Anwendungen genutzt. Das Guthaben (GUT) kann an Aufbuchungsstellen (KA, HO) erhöht und an Abbuchungsstellen (FA) erniedrigt werden. Die in der Chipkarte (CHK) gespeicherten Guthaben (GUT) sind durch mindestens ein jeweils von bestimmten Kommunikationspartnern erzeugbares Zertifikat (CER) gesichert.



DE 41 19 924 A 1

Beschreibung

Die Prozessorchipkarte ist für eine Vielzahl von Anwendungen — z. B. POS-Banking, Rechnerzugang, Telefonkarte — geeignet. Beschränkt man sich auf die Anwendungen der Chipkarte als Zahlungsmittel, dann können prinzipiell zwei Anwendungsarten unterschieden werden:

- die Kreditanwendung; dabei werden beim Warenaustausch Buchungsdaten, wie z. B. Kontonummern ausgetauscht und Überweisungsaufträge erteilt
- die Debitanwendung; dabei werden beim Warenaustausch geldwerte Informationen aus der Karte "entnommen", z. B. werden bei der Telefonkarte bereits beim Kartenerwerb bezahlte, auf der Karte gespeicherte Gebühreneinheiten gelöscht. Sind alle Gebühreneinheiten gelöscht, dann ist die Karte wertlos und wird entsorgt.

Um die Anwendung der Chipkarte im Debitbereich preisgünstiger zu gestalten, gibt es Verfahren, mit denen man bestimmte Bereiche der Chipkarte wieder aufladen kann. "Verbrauchte" Chipkarten werden dem ausgebenden Institut zurückgegeben. Diese Institute verfügen über die Kenntnis und die Fähigkeit, die Chipkarten wieder mit geldwerter Information zu laden.

Ein solches Vorgehen ist aber verhältnismäßig umständlich. Solche Debit-Chipkarten dürften deshalb auf Akzeptanzprobleme stoßen. Anzustreben ist eine Chipkarte für Debit-Anwendungen, die jederzeit an einer Vielzahl von Aufladestationen — z. B. bei Banken, Händlern etc. — wieder aufgeladen werden können.

Die der Erfindung zugrundeliegende Aufgabe ist es, ein Verfahren aufzuzeigen, das für Guthaben in Chipkarten, die an einer Aufladestation immer wieder mit geldwerter Information geladen werden können, ein Höchstmaß an Sicherheit bietet. Dazu soll die Chipkarte jede Manipulation an der Chipkarte selbst wirksam verhindern und Manipulationen an den Aufbuchungs- und Abbuchungsstellen erkennen können.

Diese Aufgabe wird durch die im Anspruch 1 angegebenen Merkmale gelöst.

Die Chipkarte arbeitet dabei z. B. nach einem in EP 9 01 13 990.7 beschriebenen Verfahren. Für verschiedene Anwendungen (z. B. Abbuchen, Aufbuchen) werden vom Kommunikationspartner in der Chipkarte gespeicherte Basisfunktionen in einer jeweils in einem Protokoll festgelegten Reihenfolge abgearbeitet. Die Einhaltung der Protokollreihenfolge wird von der Chipkarte selbst überwacht. Welches Anwendungsprotokoll maßgebend ist, wird bei der Initialisierung der Kommunikationspartner festgelegt. Die Initialisierung erfolgt nach erfolgter elektrischer, elektromagnetischer oder optischer Verbindung der Kommunikationspartner. Praktisch ist damit z. B. ausgeschlossen, daß an einer Abbuchungsstelle eine Aufbuchung stattfindet und umgekehrt.

Zusätzlich wird durch eine gegenseitige oder auch einseitige Authentifikation sichergestellt, daß nur einander bekannte Kommunikationspartner miteinander Daten austauschen. Für eine Authentifikation ist eine eindeutige Identifizierbarkeit der Kommunikationspartner Voraussetzung. Diese ist zum Beispiel durch Vergabe von Nummern (Chipkartennummer, Abbuchungsstellennummer, Aufbuchungsstellennummer) erreichbar. Des weiteren müssen, um eine Authentifikation durchführen zu können, zwischen den Kommunikationspartnern kryptografische Schlüssel vereinbart sein. Je nach den technischen Möglichkeiten der einzelnen Kommunikationspartner sind diese Schlüssel für symmetrische oder asymmetrische Verschlüsselung vereinbart. Bei symmetrischer Verschlüsselung ist speziell für jedes mögliche Paar von Kommunikationspartnern ein Schlüssel vereinbart. Bei asymmetrischer Verschlüsselung ist jedem Kommunikationspartner ein geheimer und ein öffentlicher Schlüssel zugeordnet. Diese Kenngrößen (spezielle Nummern und Schlüssel) können gemäß dem vorliegenden Verfahren zusätzlich zur Sicherung der ladbaren Guthaben in der Chipkarte verwendet werden. Es versteht sich, daß auch speziell für diese Sicherung des Guthabens Nummern und Schlüssel vereinbart werden können. Anzumerken ist auch, daß sich die Kenngrößen nur auf die verwendeten Kommunikationspartner beziehen. Rückschlüsse auf den Benutzer einer Chipkarte sind damit von vornherein stets ausgeschlossen.

Wird die Chipkarte mit einer Aufbuchungs- bzw. Abbuchungsstelle verbunden und ist die Authentizität der Kommunikationspartner festgestellt, dann fordert die Aufbuchungsstelle bzw. die Abbuchungsstelle das in der Chipkarte gespeicherte Guthaben und ein oder mehrere dazugehörige(s) ebenfalls gespeicherte(s) Zertifikat(e) an.

Ein Zertifikat wird mit Hilfe eines Verschlüsselungsalgorithmus nach der Beziehung

Zertifikat = f (Schlüssel, Guthaben),

bestimmt.

Ein Zertifikat kann demzufolge nur von demjenigen Kommunikationspartner berechnet werden, der den Schlüssel und das Guthaben kennt und den Verschlüsselungsalgorithmus ausführen kann. Dies gilt bei Verwendung eines symmetrischen Verschlüsselungsalgorithmus (z. B. DES (Data-Encryption-Standard)) auch für die Überprüfung des Zertifikates. Bei Verwendung von asymmetrischen Verschlüsselungsverfahren (z.B RSA) kann jeder, der den Verschlüsselungsalgorithmus ausführen kann, anhand des öffentlichen Schlüssels und des Guthabens die Echtheit des Zertifikats und damit die Gültigkeit des übermittelten Guthabens überprüfen.

Nach erfolgreichem Vergleich des aus Schlüssel und Guthaben in der Aufbuchungsstelle oder Abbuchungsstelle bestimmten Zertifikates mit dem aus der Chipkarte angeforderten Zertifikat kann das Guthaben verändert werden. Handelt es sich beim Kommunikationspartner um eine Aufbuchungsstelle, so wird das Guthaben erhöht. Handelt es sich um eine Abbuchungsstelle, dann wird das Guthaben vermindert.

Das Guthaben mit Zertifikat kann auf unterschiedliche Art und Weise verändert werden:

1. Die Aufbuchungsstelle bzw. Abbuchungsstelle addiert bzw. subtrahiert einen Geldbetrag zum Guthaben. Zu dem sich aus der Addition bzw. Subtraktion ergebenden neuen Guthaben berechnet die Aufbuchungsstelle bzw. Abbuchungsstelle ein oder mehrere neue(s) Zertifikat(e). Diese(s) Zertifikat(e) übermittelt sie gemeinsam mit dem neuen Guthaben zur Chipkarte.
2. Die Aufbuchungsstelle bzw. Abbuchungsstelle bestimmt wie bei 1. die/das Zertifikat(e). Das neue Guthaben wird aber auf der Chipkarte selbst errechnet. In diesem Falle entfällt die Übertragung

des neuen Guthabens von der Aufbuchungsstelle bzw. Abbuchungsstelle zur Chipkarte.

3. Die Aufbuchungsstelle bzw. Abbuchungsstelle bestätigt der Chipkarte die Echtheit des Guthabens durch Übermitteln einer entsprechenden Nachricht. In der Chipkarte wird dadurch eine Funktion angeregt, die es der Chipkarte erlaubt, das neue Guthaben selbst zu berechnen, und das/die neue(n) Zertifikat(e) selbständig zu bestimmen.

4. Die Aufbuchungsstelle bzw. die Abbuchungsstelle addiert bzw. subtrahiert einen Geldbetrag zum bzw. vom Guthaben. Zum resultierenden neuen Guthaben bestimmt die Abbuchungsstelle wenigstens ein neues Zertifikat. Dieses neue Zertifikat wird zur Chipkarte übertragen. Die Chipkarte erhält gemeinsam mit dem Zertifikat das neue Guthaben mitgeteilt oder errechnet es selbst. Aus dem neuen Guthaben und einem weiteren Schlüssel bestimmt die Chipkarte mindestens ein weiteres neues Zertifikat.

Das neue Guthaben mit allen neuen Zertifikaten und eventuell auch die Nummern der beteiligten Kommunikationspartner wird als Buchungssatz zumindest in der Chipkarte gespeichert. Aus diesem Buchungssatz kann später nachvollzogen werden, welche Kommunikationspartner miteinander geldwerte Information ausgetauscht haben.

Mit dem erfindungsgemäßen Verfahren wird ein umfassender Schutz für ladbare Guthaben auf Chipkarten oder sonstigen tragbaren Datenträgern erreicht. Buchungen können nur gemeinsam mit authentisierten Kommunikationspartnern wirksam durchgeführt werden. Nur Guthaben mit richtigen Zertifikaten werden als gültig anerkannt. Es ist für eine übergeordnete Stelle anhand der gespeicherten Buchungssätze möglich, festzustellen, wer mit wem kommuniziert hat und welcher Kommunikationspartner möglicherweise manipuliert war.

Gemäß einer Weiterbildung und Ausgestaltung des Verfahrens wird das Guthaben in der Chipkarte in Form einer Mehrzahl von Gutscheinen eines bestimmten Nominalwertes gespeichert. Jedem Gutschein wird ein Zertifikat angefügt. Bei dieser Ausführungsform eignet sich die Verwendung eines asymmetrischen Verschlüsselungsverfahrens zur Zertifikatbestimmung besonders gut.

Die Aufbuchungsstelle erzeugt mit einem geheimen Schlüssel, der auch kartenspezifisch sein kann, die Zertifikate zu den einzelnen Gutscheinen. Nach obigem Verfahren werden eine Mehrzahl von Gutscheinen mit Zertifikat in der Chipkarte gespeichert. Die Abbuchungsstelle vergewissert sich, daß ausreichend echte Guthaben in der Chipkarte gespeichert sind, indem sie die Zertifikate mit einem passenden öffentlichen Schlüssel überprüft. Zur Verringerung des Guthabens auf der Chipkarte werden lediglich eine entsprechende Anzahl Gutscheine auf der Chipkarte ungültig gemacht.

Diese Weiterbildung gewährleistet, daß auf der Chipkarte kein Restbetrag entstehen kann, daß keine geheimen Schlüssel außerhalb der Aufbuchungsstelle vorhanden sein müssen, und dennoch ausreichend gesicherte überprüfbare Guthaben auf der Chipkarte gespeichert werden können.

Weitere Ausgestaltungen und Weiterbildungen des erfindungsgemäßen Verfahrens sind in weiteren Unteransprüchen angegeben.

Ein Ausführungsbeispiel der Erfindung wird anhand der Zeichnung näher erläutert. Es zeigen:

Fig. 1 eine prinzipielle Ablaufdarstellung des erfindungsgemässen Verfahrens,

Fig. 2 die Kommunikationspartner, die an einer speziellen Ausführungsform des Verfahrens beteiligt sind,

Fig. 3 ein Schaubild, in dem dargestellt ist, wer in der speziellen Ausführungsform aus **Fig.** 2 welches Zertifikat bestimmen kann,

Fig. 4 ein Protokoll zum Aufbuchen des Guthabens einer Chipkarte nach dem Ausführungsbeispiel gemäß **Fig.** 2 und

Fig. 5 ein Protokoll zum Abbuchen des Guthabens einer Chipkarte nach dem Ausführungsbeispiel gemäß **Fig.** 2.

In **Fig.** 1 ist eine prinzipielle Ablaufdarstellung des erfindungsgemäßen Verfahrens dargestellt. Neben einem Block, der eine Chipkarte CHK repräsentiert, erscheint ein Block, der eine Aufbuchungsstelle KA, HO bzw. eine Abbuchungsstelle FA darstellt. In einer Abfolge von oben nach unten verlaufen mehrere Pfeile zwischen den beiden Blöcken. Der erste Pfeil symbolisiert die Initialisierung INIT, die im Anschluß an die elektrische Verbindung der beiden Kommunikationspartner erfolgt. In Anschluß an die Initialisierung INIT ist der Kommunikationspartner für die Chipkarte CHK bekannt und auf der Chipkarte kann infolgedessen ein speziell für diesen Kommunikationspartner gültiges Protokoll abgearbeitet werden. Dieses Protokoll sieht zunächst eine gegenseitige Authentifikation AUTH zwischen Chipkarte CHK und Kommunikationspartner FA, KA, HO vor. Erst wenn die Authentifikation AUTH, beispielsweise nach dem Challenge- and Response-Verfahren, erfolgreich beendet ist, werden Daten DAT von der Chipkarte CHK zum Kommunikationspartner FA, KA, HO übertragen. Die zu übertragenden Daten DAT werden vorher durch einen Message Authentication Code MAC gesichert. Der MAC wird gemeinsam mit einem Guthaben GUT und wenigstens einem Zertifikat CER zum Kommunikationspartner FA, KA, HO übertragen. Im Kommunikationspartner erfolgt eine Überprüfung CHEK der übertragenen Daten DAT anhand des MAC und anschließend des übertragenen Guthabens GUT anhand des Zertifikates CER. Nach erfolgreicher Überprüfung CHEK errechnet der Kommuniaktionspartner FA, KA, HO ein neues Guthaben NGUT und mindestens ein dazugehöriges neues Zertifikat NCER. Zu diesem neuen Guthaben NGUT und dem neuen Zertifikat NCER errechnet der Kommunikationspartner FA, KA, HO einen MAC und überträgt diese Daten DAT anschließend zur Chipkarte CHK. Die Chipkarte CHK bestimmt unter Umständen ein weiteres neues Zertifikat NCER, und fügt es den übertragenen Daten an. Der Auf- oder Abbuchungsvorgang ist damit beendet und die Chipkarte CHK kann wieder vom Kommunikationspartner FA, KA, HO getrennt werden.

Fig. 2 zeigt die Komponenten, die bei einer speziellen Ausführungsform des Verfahrens benötigt werden. Diese spezielle Ausführungsform beschreibt die Verwendung der Chipkarte CHK zum Kauf von Fahrscheinen T für öffentliche Verkehrsmittel. Ein Kunde KU ist Besitzer einer Chipkarte CHK. Um diese Chipkarte CHK mit einem Geldbetrag BETR zu laden, begibt er sich zu einem Händler. Dieser Händler verfügt über eine Händlerkasse KA, die über eine Datenübertragungsleitung DÜ mit einem Host-Rechner HO verbindbar ist. Die Händlerkasse KA und der Host-Rechner HO verkörpern die Aufbuchungsstelle. Nach erfolgter Aufbuchung

der Chipkarte CHK erhält der Kunde KU ein Journal J, auf dem der Händler die Aufbuchung des Geldbetrages BETR auf der Chipkarte CHK bestätigt. Mit dieser Chipkarte CHK kann nun der Kunde KU bei jedem, dem öffentlichen Verkehrssystem zugehörigen Fahrscheinautomaten FA einen Fahrschein T erwerben. Der Fahrkartenautomat FA verkörpert dabei die Abbuchungsstelle. Der Fahrkartenautomat FA arbeitet Off-Line.

Die Sicherung der Guthaben GUT auf den zu dem in **Fig.** 2 dargestellten öffentlichen Verkehrssystem gehörigen Chipkarten CHK wird in **Fig.** 3 veranschaulicht. Jedem Guthaben GUTX, GUTY werden zwei vom Guthaben GUTX, GUTY abhängige Zertifikate CER(X)CHKA, CER(X)FA bzw. CER(Y)CHKB, CER(Y)FA angefügt. Durch Pfeile ist in **Fig.** 3 verdeutlicht, welcher Kommunikationspartner CHKA, CHKB, HO, FA welches Zertifikat CER bestimmen kann. Demnach ist der Host-Rechner HO in der Lage, sämtliche Zertifikate CER zu bestimmen. Der Fahrscheinautomat FA kann die Fahrkartenautomatenzertifikate CER(X)FA, CER(Y)FA bestimmen, und jede Chipkarte CHKA bzw. CHKB kann jeweils nur ihr kartenspezifisches Zertifikat CER(X)CHKA bzw. CER(Y)CHKB bestimmen.

Im einzelnen werden die Zertifikate CER durch folgende Gleichungen bestimmt:

$$CER(X)CHKA = f(K(A), GUTX)$$
$$CER(Y)CHKB = f(K(B), GUTY)$$
$$CER(X)FA = f(K(FA), GUTX)$$
$$CER(Y)FA = f(K(FA), GUTY)$$

In diesem hier beispielhaft aufgezeigten symmetrischen Verschlüsselungsverfahren werden geheime, jeweils zwischen zwei Kommunikationspartnern gültige Schlüssel K verwendet. Die Schlüssel K für die kartenspezifischen Zertifikate CER(X)CHKA bzw. CER(Y)CHKB ihrerseits werden durch eine sogenannte Einwegfunktion g (keine Umkehrfunktion vorhanden) aus einem geheimen Schlüssel K' einer Chipkartennummer CHKNR nach der Beziehung

$$K(A) = g(K', CHKNR(A))$$
$$K(B) = g(K', CHKNR(B))$$

gebildet.

Die geheimen Schlüssel K' können jeweils für mehrere Chipkarten CHK identisch sein. Die Einwegfunktion g muß nicht in jedem Kommunikationspartner ausgeführt werden. Es genügt, wenn lediglich der Host-Rechner HO diese Einwegfunktion g ausführen kann. In den Chipkarten CHK kann jeweils der Chipkartenschlüssel K(A), K(B) direkt gespeichert und verwendet werden.

Um einen weitergehenden Schutz des Guthabens GUT zu erzielen, z. B. einen Schutz gegen Wiedereinspielen des Automatenzertifikates CER(X)FA, CER(Y)FA, kann dieses Zertifikat CER(X)FA, CER(Y)FA, auch kartenspezifisch nach folgender Gleichung bestimmt werden:

$$CER'(X)FA = F(K(FA), GUTX, CHKNR(A))$$
$$CER'(Y)FA = F(K(FA), GUTY, CHKNR(B))$$

Anhand der **Fig.** 4a bis 4g werden im folgenden die Verfahrensabläufe beim Aufbuchen einer Chipkarte CHK, die in einem System gemäß den **Fig.** 2 und 3 verwendet wird, dargelegt. Der Verfahrensablauf ist eine Abfolge einzelner Funktionen. Die am Aufbuchungsvorgang beteiligten Systemkomponenten sind:

- eine Chipkarte CHK
- eine Händlerkasse KA mit Sicherheitsmodul KASM
- ein Host-Rechner HO mit Sicherheitsmodul HOSM.

Die Sicherheitsmodule KASM bzw. HOSM sind besonders geschützte Bereiche innerhalb der Händlerkasse KA bzw. des Host-Rechners HO. Für jede Systemkomponente ist in der Figur eine Spalte vorgesehen. Da die Händlerkasse KA sowohl mit dem Host-Rechner HO als auch mit der Chipkarte CHK kommuniziert, sind für die Händlerkasse KA aus Gründen der Übersichtlichkeit zwei Spalten vorgesehen. Jede Funktion wird durch einen rechteckigen Rahmen symbolisiert. Die Funktionen sind fortlaufend numeriert. Ein Pfeil oberhalb des rechteckigen Rahmens zeigt, aus welcher Systemkomponente die Eingangsdaten der Funktion stammen. Ein Pfeil unterhalb des rechteckigen Rahmens zeigt an, wem die Ausgangsdaten der Funktion übermittelt werden.

Anhand der Funktionsnumerierung wird der Verfahrensablauf nun stichwortartig beschrieben:

A: Initialisierung

1. Chipkarte CHK und Händlerkasse KA werden in einen Grundzustand RES versetzt.
2. Die Händlerkasse KA bestimmt ein Anwendungsdatenfeld ADF (Application Data Field). Dadurch wird das maßgebliche Protokoll SELPRO in der Chipkarte CHK gewählt. Die Chipkarte CHK quittiert dies durch Übertragen eines Statussignals STA.
3. Die Händlerkasse KA übermittelt eine Blocknummer BNR(A). Dadurch wird eine bestimmte Speicherstelle in der Chipkarte CHK durch die Funktion READ gelesen. Die Chipkarte CHK übermittelt die gelesene Kartennummer CHKNR an die Händlerkasse KA.
4. Die Händlerkasse KA überträgt eine Blocknummer BNR(D). Dadurch wird ein Buchungszählerstand BZ in der Chipkarte CHK gelesen und zur Händlerkasse KA übertragen.
5. Die Händlerkasse KA übermittelt dem Händlerkassensicherheitsmodul KASM einen Anwendungsnamen AN. Dadurch wird ein Protokoll SELPRO gewählt. Das Händlerkassensicherheitsmodul KASM quittiert durch ein Statussignal STA.

B: Gegenseitige Authentifikation AUTH, Chipkarte CHK — Händlerkasse KA

6. Das Händlerkassensicherheitsmodul KASM generiert eine erste Zufallszahl V.
7. Die Händlerkasse KA ruft mit dem Signal CALA und der Übertragung der ersten Zufallszahl V eine Funktion CALAP zur Berechnung eines Anerkennungsparameters AP auf. Dieser Anerkennungsparameter AP wird von der Chipkarte CHK zur Händlerkasse KA übertragen.
8. Die Händlerkasse KA ruft durch die Übertragung des Signals CALA, der Chipkartennummer CHKNR und des Anerkennungsparameters AP eine Funktion AUTHCHK zur Authentifikation der Chipkarte CHK im Kassensicherheitsmodul

KASM auf. Das Kassensicherheitsmodul KASM quittiert die Richtigkeit des Anerkennungsparameters AP.

9. Die Chipkarte CHK erzeugt mit Hilfe ihres Zufallsgenerators GENRAN eine zweite Zufallszahl V' und überträgt diese an die Händlerkasse KA.

10. Die Händlerkasse KA überträgt ein Signal CALA und die zweite Zufallszahl V' an das Händlerkassenmodul KASM. Dadurch wird die Funktion zur Berechnung des Anerkennungsparameters AP' aufgerufen, dieser Anerkennungsparamter AP' liegt der Händlerkasse KA vor.

11. Die Händlerkasse KA überträgt ein Signal CALA und den zweiten Anerkennungsparameter AP' an die Chipkarte CHK. Dadurch wird eine Funktion AUTHKA zur Authentifikation AUTH der Händlerkasse KA aufgerufen. Die Chipkarte CHK bestätigt die Richtigkeit des zweiten Anerkennungsparameters AP' durch eine Quittung OK.

C: Herstellen der On-Line-Verbindung zum Host-Rechner HO

12. Die Händlerkasse KA überträgt eine Blocknummer BNR(C) an die Chipkarte CHK. Dadurch wird die Lesefunktion READ aufgerufen und das aktuelle Guthaben GUT und das Zertifikat CERFA an die Händlerkasse KA übertragen.

13. Die Händlerkasse KA übermittelt ein Signal CALM und Daten DAT1, die mindestens das Guthaben GUT und das fahrscheinautomatenspezifische Zertifikat CERFA umfassen an das Händlerkassensicherheitsmodul KASM. Dadurch wird eine Funktion CALMAC zur Berechnung eines Message Authentificationcodes MAC gestartet. Der MAC und die Daten DAT1 werden zum Host-Rechner HO übertragen.

14. Im Host-Rechner-Sicherheitsmodul HOSM wird durch Übertragung des Anwendungsnamens AN das Protokoll SELPRO gewählt. Das Host-Rechner-Sicherheitsmodul HOSM quittiert es durch ein Statussignal STA.

15. Der Host-Rechner HO überträgt ein Signal CALK und eine Händlernummer KANR an das Händlerkassensicherheitsmodul HOSM. Dadurch wird eine Schlüsselberechnungsfunktion CALKEY gestartet. Nach erfolgreicher Abarbeitung der Funktion CALKEY erhält der Host-Rechner HO eine Quittung OK.

16. Übertragung eines Signals CHECKM und der Daten DAT1 zum Host-Rechner-Sicherheitsmodul HOSM. Dadurch Aufruf einer Überprüfungsfunktion CHECKMAC für den MAC und Quittung OK an Host-Rechner HO.

17. Generierung einer Zufallszahl V im Zufallszahlengenerator GENRAN des Host-Rechner-Sicherheitsmoduls HOSM und Übertragung der Zufallszahl V an die Händlerkasse KA.

18. Aufruf der Schlüsselberechnungsfunktion CALKEY im Händlerkassensicherheitsmodul KASM durch Übertragung eines Signals CALK und der Chipkartennummer CHKNR von der Händlerkasse KA zum Händlerkassensicherheitsmodul KASM sowie Quittung OK an Händlerkasse KA.

19. Übertragung des Signals CALM und eines Geldbetrags BETR von der Händlerkasse KA zum Händlerkassensicherheitsmodul KASM. Dadurch Start der Funktion CALMAC zur Berechnung eines MAC und Übertragung des MAC an die Händlerkasse KA.

20. Übertragung des Signals CHECKM, des Geldbetrags BETR und des MAC von der Händlerkasse KA zur Chipkarte CHK. Dadurch Start der Überprüfungsfunktion CHECKMAC für MAC und Quittung OK an Händlerkasse KA.

D: Gegenseitige Authentifikation AUTH, Händlerkasse KA – Host-Rechner HO

21. Funktion CALAP zur Berechnung des Anerkennungsparameters AP wird durch das Signal CALA und die Zufallszahl V aufgerufen.

22. Im Händlerkassensicherheitsmodul KASM wird eine Zufallszahl V' generiert und gemeinsam mit dem Anerkennungsparameter AP zum Host-Rechner HO übertragen.

23. Funktion AUTHKA im Host-Rechner-Sicherheitsmodul HOSM wird durch das Signal CALA die Händlerkassennummer KANR und den Anerkennungsparameter AP aufgerufen. Es erfolgt Quittung OK.

24. Durch das Signal CALA und die Zufallszahl V' wird Funktion CALAP zur Berechnung eines weiteren Anerkennungsparameters AP' gestartet.

25. Im Host-Rechner-Sicherheitsmodul HOSM wird eine weitere Zufallszahl V erzeugt und gemeinsam mit dem Anerkennungsparameter AP' an die Händlerkasse KA übertragen.

26. Durch das Signal CALA und den Anerkennungsparameter AP' wird im Händlerkassensicherheitsmodul KASM die Funktion AUTHHO zur Authentifikation des Host-Rechners HO gestartet. Quittung OK an Händlerkasse KA.

E: Gegenseitige Authentifikation AUTH, Chipkarte CHK – Host-Rechner HO

27. Start der Funktion CALAP durch Übertragung des Signals CALA und der vom Host-Rechner HO erzeugten Zufallszahl V an die Chipkarte CHK. Übertragung des Anerkennungsparameters AP an Händlerkasse KA.

28. Zufallszahlengenerator GENRAN der Chipkarte CHK generiert eine Zufallszahl V'. Diese wird über die Händlerkasse KA gemeinsam mit dem Anerkennungsparameter AP zum Host-Rechner HO übertragen.

29. Funktion AUTHCHK zur Authentifikation der Chipkarte CHK im Host-Rechner-Sicherheitsmodul HOSM wird durch das Signal CALA, die Chipkartennummer CHKNR und den Anerkennungsparameter AP gestartet. Quittung OK an Host-Rechner HO.

30. Funktion CALAP zur Berechnung eines neuen Anerkennungsparameters AP' wird durch das Signal CALA und die Zufallszahl V' gestartet.
Überprüfung, ob eine Sperre SP für die Chipkarte CHK vorliegt; wenn ja: Fortsetzung mit den Schritten Nummer 32a – 32f. Andernfalls Übertragung des Anerkennungsparameters AP' an Händlerkasse KA.

31. Funktion AUTHHO zur Authentifikation des Host-Rechners HO wird durch das Signal CALA und den Anerkennungsparameter AP' in der Chipkarte CHK gestartet, Quittung OK an Händlerkasse. Fortsetzung mit Schritt Nummer 33.

F: Abbruch der Anwendung bei vorliegender Sperre SP für Chipkarte CHK

32a. Generierung einer Zufallszahl V• im Host-Rechner-Sicherheitsmodul HOSM und Übertragung dieser Zufallszahl V• und des zuletzt errechneten Anerkennungsparameters AP' an Händlerkasse KA.
32b. Aufruf der Funktion CHKSP zum Sperren der Chipkarte durch Übertragen des Anerkennungsparameters AP' und der Zufallszahl V• an die Chipkarte CHK. Chipkarte überträgt daraufhin einen weiteren Anerkennungsparameter AP• an Host-Rechner HO.
32c. Aufruf der Funktion AUTHCHK zur Authentifikation AUTH der Chipkarte CHK durch das Signal CALA und den Anerkennungsparameter AP•. Quittung OK an Host-Rechner HO.
32d. Übertragung der Quittung OK an Händlerkasse und Beenden der Anwendung CLPRO im Host-Rechner HO.
32e. Beenden der Anwendung CLPRO in der Händlerkasse KA, Abgabe eines Quittungssignals OK an Chipkarte CHK.
32f. Beenden der Anwendung CLPRO in der Chipkarte CHK.

G: Überprüfung des Guthabens GUT im Host-Rechner HO

33. Die Schritte 32a – 32f wurden ausgelassen, die Händlerkasse überträgt Blocknummern BNR(B), BNR(C) an die Chipkarte CHK. In der Chipkarte werden Daten DAT2, die das Guthaben GUTH, ein kartenspezifisches Zertifikat CERCHK und ein fahrscheinautomatenspezifisches Zertifikat CERFA umfassen, gelesen und ein MAC dazu erstellt. DAT2 und MAC werden an die Händlerkasse KA übertragen.
34. Im Zufallsgenerator GENRAN der Chipkarte CHK wird eine Zufallszahl V erzeugt und an die Händlerkasse KA übertragen. Die Händlerkasse KA überträgt die Daten DAT2, den MAC und die Zufallszahl V an den Host-Rechner HO.
35. Aufruf der Schlüsselberechnungsfunktion CALKEY durch das Signal CALK und die Chipkartennummer CHKNR. Quittung OK an Host-Rechner HO.
36. Aufruf der Überprüfungsfunktion CHECKMAC durch Übermittlungssignal CHECKM, die Daten DAT2 und den MAC. Quittung OK an Host-Rechner HO.
37. Aufruf der Funktion CHECKCER zur Überprüfung des Fahrkartenautomatenzertifikates CERFA durch Übermittlung eines Signals CHECKC, durch das Guthaben GUT und das Zertifikat CERFA. Quittung OK an Host-Rechner HO.
38. Aufruf der Schlüsselberechnungsfunktion CALKEY durch das Signal CALK und die Chipkartennummer CHKNR. Quittung OK an Host-Rechner HO.
39. Aufruf der Überprüfungsfunktion CHECKCER für das chipkartenspezifische Zertifikat CERCHK durch Übermittlung des Signals CHECKC, durch das Guthaben GUT und das Zertifikat CERCHK. Quittung OK an Host-Rechner HO.

H: Erstellen des neuen Guthabens NGUT

40. Aufruf einer Zertifikatsberechnungsfunktion CALCER durch ein Signal CALC und des neue Guthaben NGUT. Neues Fahrkartenautomatenzertifikat NCERFA an Host-Rechner HO.
41. Aufruf der Schlüsselberechnungsfunktion CALKEY durch das Signal CALK und die Chipkartennummer CHKNR. Quittung OK an Host Rechner HO.
42. Aufruf der Zertifikatsberechnungsfunktion CALCER durch das Signal CALC und das neue Guthaben NGUT. Übertragung des neuen chipkartenspezifischen Zertifikats NCERCHK an Host-Rechner HO.
43. Aufruf Schlüsselberechnungsfunktion CALKEY durch Signal CALK und Chipkartennummer CHKNR. Quittung OK an Host-Rechner HO.
44. Aufruf Funktion CALMAC zur Berechnung des MAC durch das Signal CALM der mit Position 34 von der Chipkarte CHK zum Host-Rechner HO übermittelten Zufallszahl V und die Daten DAT3, die unter anderem die beiden neuen Zertifikate NCERCHK und NCERFA umfassen. Der errechnete MAC und die Daten DAT3 werden an die Händlerkasse KA übermittelt.

I: Chipkarte CHK aufbuchen und Anwendung beenden

45. Aufruf der Überprüfungsfunktion CHECKMAC zur Überprüfung des MAC durch das Signal CHECKM, die Daten DAT3 und den MAC. Anschließend Speichern des neuen Guthabens NGUT und der beiden neuen Zertifikate NCERFA, NCERCHK. Quittung OK an Händlerkasse KA und Host-Rechner HO.
46. Aufruf der Funktion "Anwendung beenden" CLPRO im Host-Rechner HO, in der Händlerkasse KA und in der Chipkarte CHK.

Anhand der **Fig.** 5a bis 5d wird im folgenden der Verfahrensablauf beim Abbuchen des Guthabens GUT einer Chipkarte CHK, die in einem System gemäß den **Fig.** 2 und 3 verwendet wird, dargelegt. Der Verfahrensablauf ist, wie beim Aufbuchen, eine Abfolge einzelner Funktionen. Die am Abbuchungsvorgang beteiligten Systemkomponenten sind:

- eine Chipkarte CHK
- ein Fahrscheinautomat FA mit Sicherheitsmodul FASM.

Der Aufbau der Figur entspricht im Prinzip der **Fig.** 4. Anhand der Funktionsnumerierung wird der Verfahrensablauf nun stichwortartig beschrieben:

A: Initialisierung INIT

1. Reset zur Erreichung des Grundzustandes RES in Chipkarte CHK und Fahrscheinautomat FA.
2. Aufruf eines Protokolls SELPRO durch Übermitteln eines Anwendungsdatenfeldes ADF an die Chipkarte CHK, Quittung durch Statussignal STA an Fahrkartenautomat FA.
3. Aufruf des Protokolls SELPRO im Fahrkartenautomat FA durch den Anwendungsnamen AN. Quittung durch Statussignal STA.
4. Übertragung einer Blocknummer BNR(A) zur

Chipkarte CHK, in der Lesefunktion READ aktiviert wird. Übertragung der Chipkartennummer CHKNR an Fahrkartenautomat FA.

B: Authentifikation AUTH

5. Generierung einer Zufallszahl V in Fahrkartenautomaten FA.
6. Aufruf der Funktion CALAP zur Berechnung des Anerkennungsparameters AP.
7. Aufruf der Funktion AUTHCHK zur Authentifikation AUTH der Chipkarte CHK durch das Signal CALA, die Chipkartennummer CHKNR und den Anerkennungsparameter AP. Quittung OK an Fahrkartenautomat FA.
8. Generieren einer Zufallszahl V' in der Chipkarte CHK.
9. Aufruf der Funktion CALAP zur Berechnung des Anerkennungsparameters AP' mit Hilfe des Signals CALA und der Zufallszahl V'.
10. Aufruf der Funktion AUTHFA zur Authentifikation AUTH des Fahrkartenautomaten FA durch das Signal CALA und den Anerkennungsparameter AP' in der Chipkarte CHK. Quittung OK an Fahrkartenautomat FA.
11. Generierung einer Zufallszahl V mit Hilfe der Funktion GENRAN im Fahrkartenautomat FA.
12. Übertragung einer Blocknummer BNR(C) und der Zufallszahl V an die Chipkarte CHK. Funktion READ liest Guthaben GUT und Fahrkartenautomatenzertifikat CERFA aus und berechnet dazu einen MAC. GUT, CERFA und MAC werden an Fahrkartenautomat FA übermittelt.
13. Aufruf der Schlüsselberechnungsfunktion CALKEY durch das Signal CALK und die Chipkartennummer CHKNR. Quittung OK an Fahrkartenautomat FA.
14. Aufruf der Überprüfungsfunktion CHECKMAC für den MAC durch das Signal CHECKM, das Guthaben GUT, das Fahrkartenautomatenzertifikat CERFA und den MAC. Quittung OK an den Fahrkartenautomaten FA.
15. Aufruf der Überprüfungsfunktion CHECKCER durch das Signal CHECKC, Quittung OK von Fahrkartenautomatensicherheitsmodul FASM an Fahrkartenautomat FA, Anzeige von Guthaben GUT am Display des Fahrkartenautomaten FA, Auswahl der Fahrscheinart durch den Kunden KU, Bestätigung durch den Kunden KU.
16. Aufruf einer Berechnungsfunktion CALGUT durch das Signal CALG und den Geldbetrag BETR. Nach Abarbeiten der Funktion liegt das neue Guthaben NGUT im Fahrkartenautomaten FA vor.
17. Aufruf Zertifikationsberechnungsfunktion CALCER durch das Signal CALC und des neue Guthaben NGUT. Es liegt das neue Fahrkartenautomatenzertifikat NCERFA vor.
18. Aufruf der Funktion CALMAC durch das Signal CALM, das neue Zertifikat NCERFA, die Fahrkartenautomatennummer FANR, das aktuelle Datum DATU und das neue Guthaben NGUT. MAC liegt im Fahrkartenautomaten FA vor.
19. Aufruf der Überprüfungsfunktion CHECKMAC in der Chipkarte CHK durch Übermitteln des Signals CHECKM, des neuen Zertifikats NCERFA, der Automatennummer FANR, des aktuellen Datums DATU und des neuen Guthabens NGUT. Quittung OK an Fahrkartenautomat FA.
20. Aufruf eines Plausibilitätstestes PLAU anhand des Guthabens GUT und des neuen Guthabens NGUT (NGUT muß kleiner sein als GUT), Quittung OK.
21. Aufruf der Berechnungsfunktion CALCER zur Berechnung des neuen chipkartenspezifischen Zertifikates NCERCHK durch das Signal CALC, anschließend Speichern der Buchung in Chipkarte CHK und Fahrkartenautomat FA.
22. Beenden der Anwendung durch Ablauf der Funktion CLPRO im Fahrkartenautomaten FA und in der Chipkarte CHK.

Patentansprüche

1. Verfahren zur Sicherung von ladbaren Guthaben in für Debitanwendungen benutzte Chipkarten, die mit Abbuchungs- und Aufbuchungsstellen über definierte, bei einer Initialisierung der Kommunikationspartner ausgewählte Protokolle nach erfolgter Authentifikation kommunizieren, mit folgenden Verfahrensschritten:

a) Übermitteln eines Datenblocks (DAT) von der Chipkarte (CHK) zur Abbuchungsstelle (FA) bzw. Aufbuchungsstelle (KA, HO), der sich mindestens zusammensetzt aus

aa) einem auf der Chipkarte (CHK) gespeicherten Guthaben (GUT)

ab) und mindestens einem, durch einen Verschlüsselungsalgorithmus aus zumindest einem zwischen den möglichen Kommunikationspartnern gültigen Schlüssel (K) und dem Guthaben (GUT) bestimmten Zertifikat (CER)

b) Überprüfen der Gültigkeit des übertragenen Guthabens (GUT) durch die Aufbuchungsstelle (KA, HO) bzw. Abbuchungsstelle (FA) mit Hilfe mindestens eines Zertifikates (CER)

c) Erstellung eines neuen Guthabens (NGUT) durch Subtraktionbzw. Addition eines Geldbetrages (BETR) zum übermittelten Guthaben (GUT)

d) Bestimmung mindestens eines neuen Zertifikats (NCER) mit Hilfe des Verschlüsselungsalgorithmus aus zumindest einem zwischen den möglichen Kommunikationspartnern gültigen Schlüssel (K) und dem neuen Guthaben (NGUT)

e) Speichern des neuen Guthabens (NGUT) oder einer entsprechenden Information und des neuen Zertifikates (NCER) zumindest in der Chipkarte (CHK).

2. Verfahren zur Sicherung nach Anspruch 1, dadurch gekennzeichnet, daß vor jeder Datenübermittlung für jeden zu übermittelnden Datenblock (DAT) ein Message-Authentifikation-Code (MAC) gebildet und anschließend zusammen mit dem Datenblock (DAT) an den Kommunikationspartner übermittelt wird.

3. Verfahren zur Sicherung nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß zum Aufbuchen des Guthabens (GUT) auf der Chipkarte (CHK) die Chipkarte (CHK) mit einem Aufbuchungsterminal (KA) verbunden wird, daß nach dem Initialisierungsvorgang (INIT) das Aufbuchungsterminal (KA) On-Line mit einem Host-Rechner (HO) verbunden wird, und daß die Über-

prüfung des Guthabens (GUT) im Host-Rechner (HO) erfolgt.

4. Verfahren zur Sicherung nach Anspruch 3, dadurch gekennzeichnet, daß der Host-Rechner (HO) die/das neue(n) Zertifikat(e) (NCER) zum neuen Guthaben (NGUT) bestimmt.

5. Verfahren zur Sicherung nach einem der vorhergehenden Ansprüche 3 oder 4, dadurch gekennzeichnet, daß zwischen jeder Chipkarte (CHK) und dem Host-Rechner (HO) ein Chipkartenschlüssel (K(A), K(B)) und zwischen den Abbuchungsstellen (FA) und dem Host-Rechner (HO) ein Abbuchungsschlüssel (K(FA)) zur Bestimmung eines Zertifikates (CER) vereinbart sind, und daß jedem Guthaben (GUT) ein mit Hilfe des Chipkartenschlüssels (K(A), K(B)) bestimmtes erstes Zertifikat (CERCHK) und ein mit Hilfe des Abbuchungsschlüssels (K(FA)) bestimmtes zweites Zertifikat (CERFA) angefügt wird.

6. Verfahren zur Sicherung nach Anspruch 5, dadurch gekennzeichnet, daß beim Abbuchungsvorgang das zweite neue Zertifikat (NCERFA) durch die Abbuchungsstelle (FA) bestimmt wird und daß das erste neue Zertifikat (NCERCHK) durch die Chipkarte (CHK) bestimmt wird.

7. Verfahren zur Sicherung nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß nach jeder Aufbuchung oder Abbuchung eines Guthabens (GUT) ein Quittungsdruck (T. J) erstellt wird.

8. Verfahren zur Sicherung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß das Guthaben (GUT) in der Chipkarte (CHK) in Form einer Mehrzahl von Gutscheinen eines bestimmten Nominalwertes gespeichert wird, und daß jedem Gutschein ein Zertifikat (CER) angefügt wird.

9. Verfahren zur Sicherung nach Anspruch 8, dadurch gekennzeichnet, daß die Abbuchungsstelle (FA) jeweils eine vom abzubuchenden Geldbetrag (BETR) bestimmte Menge Gutscheine auf der Chipkarte (CHK) ungültig macht.

10. Verfahren zur Sicherung nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß vor dem Erstellen eines neuen Guthabens (NGUT) eine Sperrdatei abgefragt wird.

Hierzu 13 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 41 19 924 A1
Int. Cl.[5]: G 06 F 15/30
Offenlegungstag: 24. Dezember 1992

FIG 1

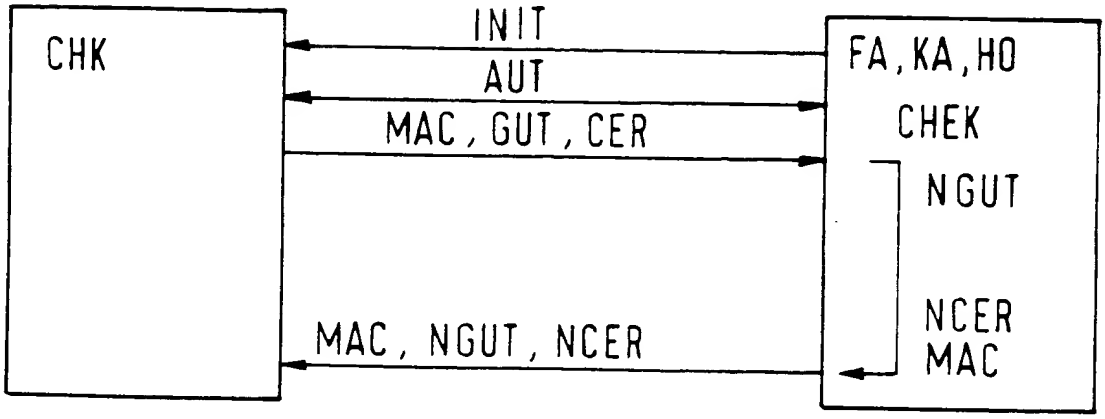
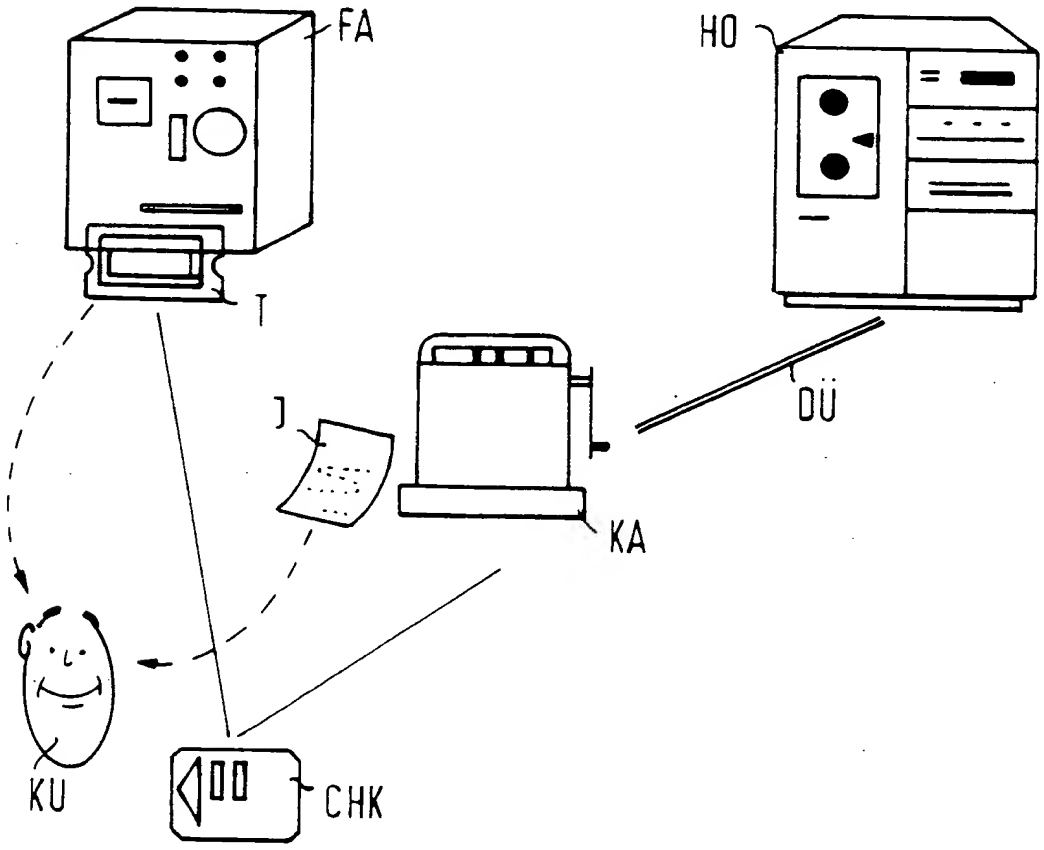
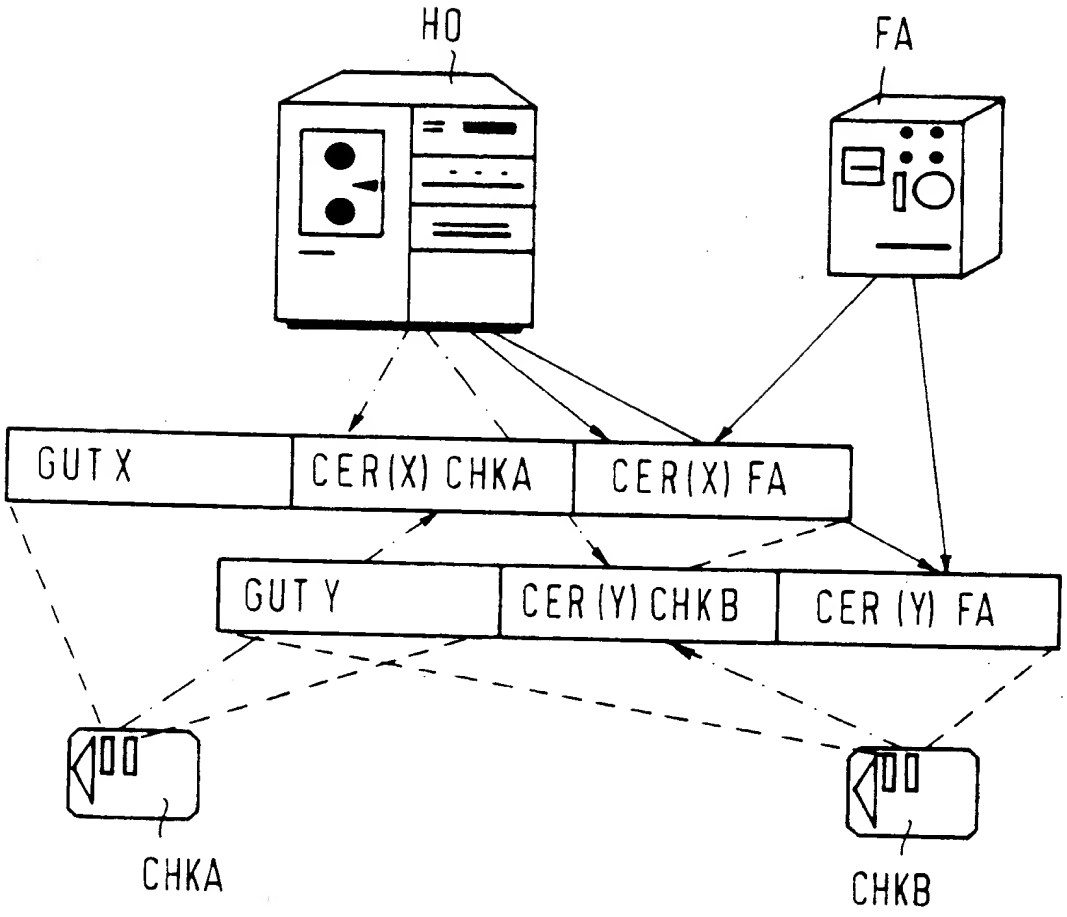


FIG 2



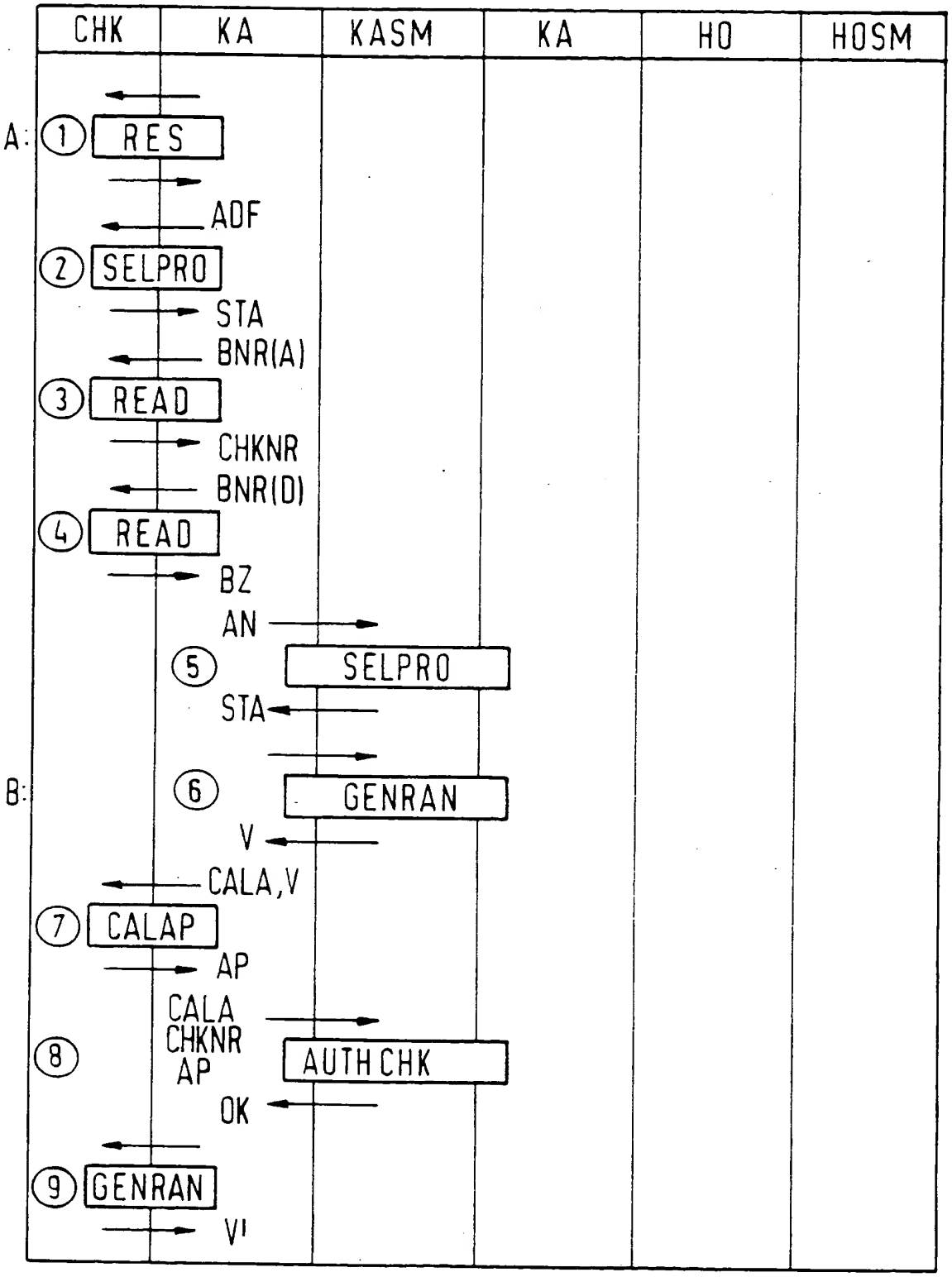
Nummer: DE 41 19 924 A1
Int. Cl.[5]: G 06 F 15/30
Offenlegungstag: 24. Dezember 1992

FIG 3



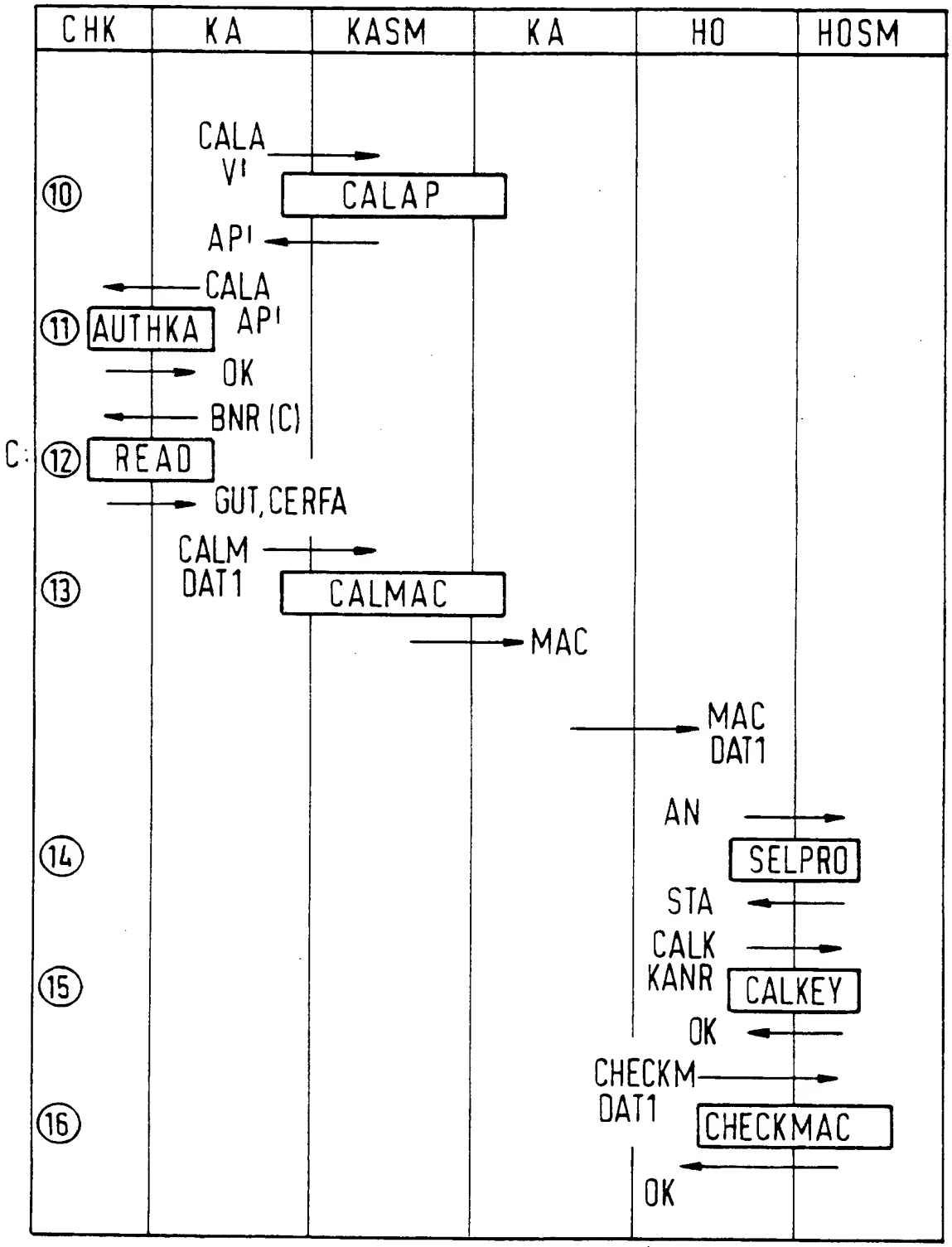
Nummer: DE 41 19 924 A1
Int. Cl.[5]: G 06 F 15/30
Offenlegungstag: 24. Dezember 1992

FIG 4a



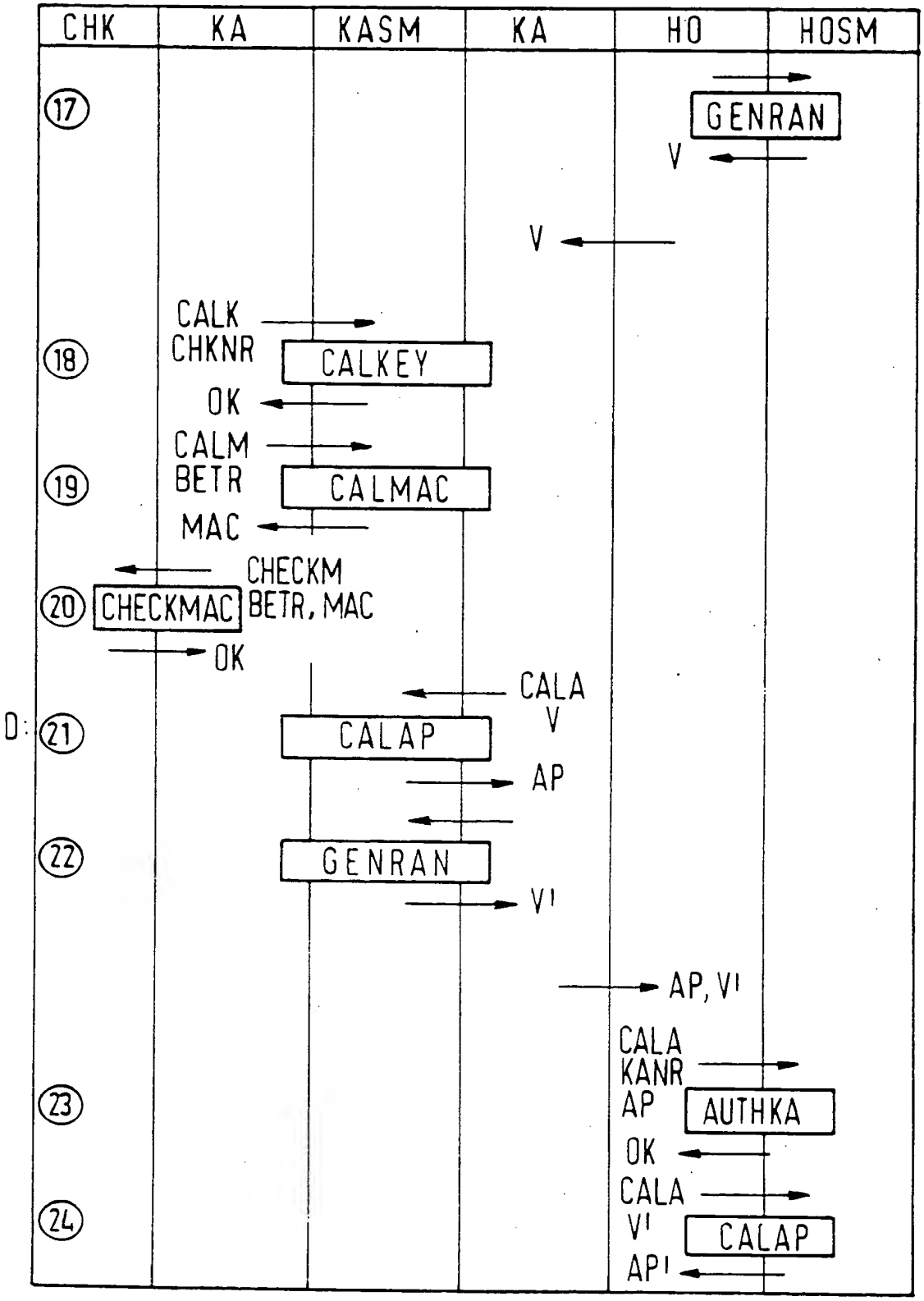
Nummer: DE 41 19 924 A1
Int. Cl.[5]: G 06 F 15/30
Offenlegungstag: 24. Dezember 1992

FIG 4b



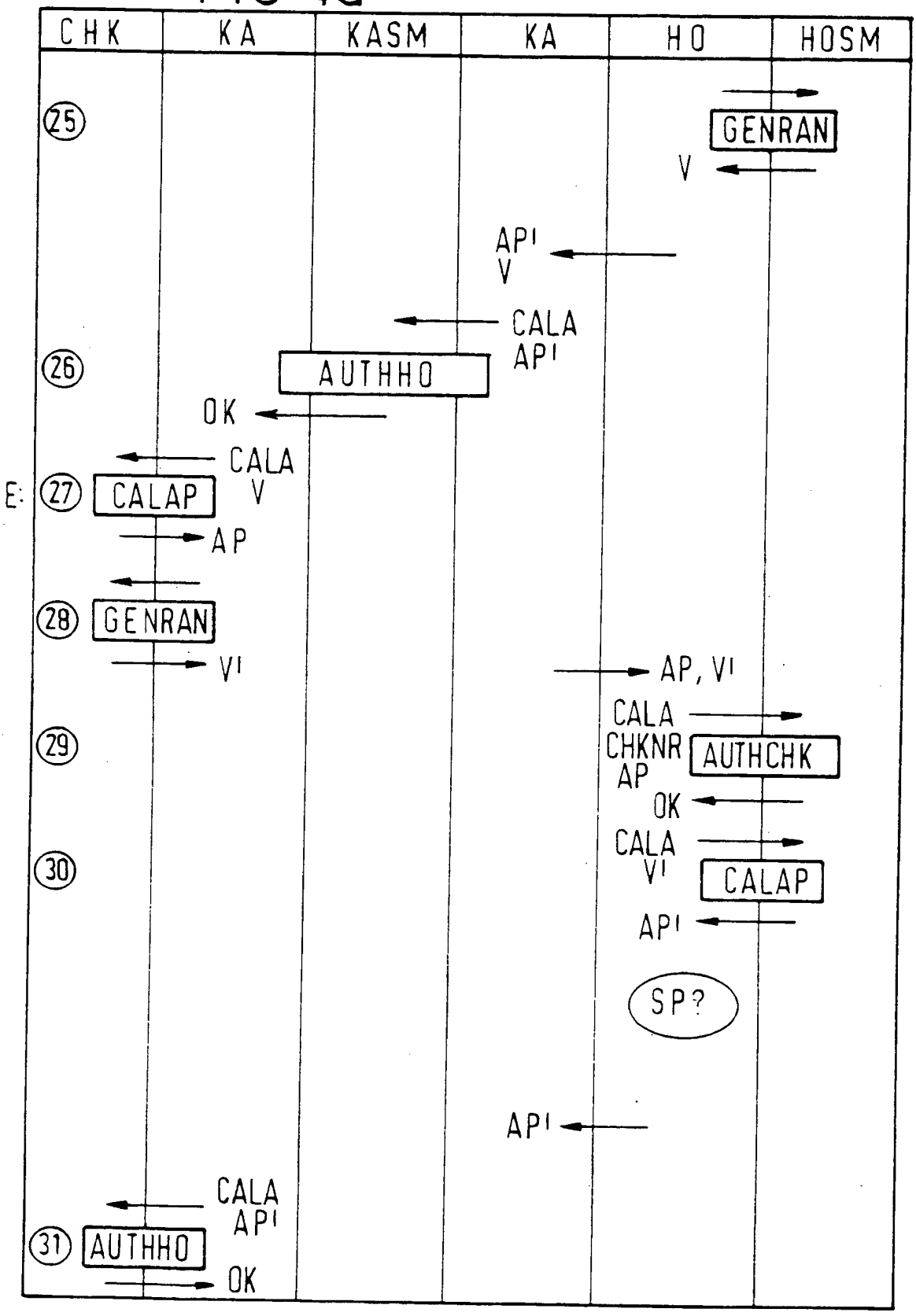
Nummer: DE 41 19 924 A1
Int. Cl.[5]: G 06 F 15/30
Offenlegungstag: 24. Dezember 1992

FIG 4c



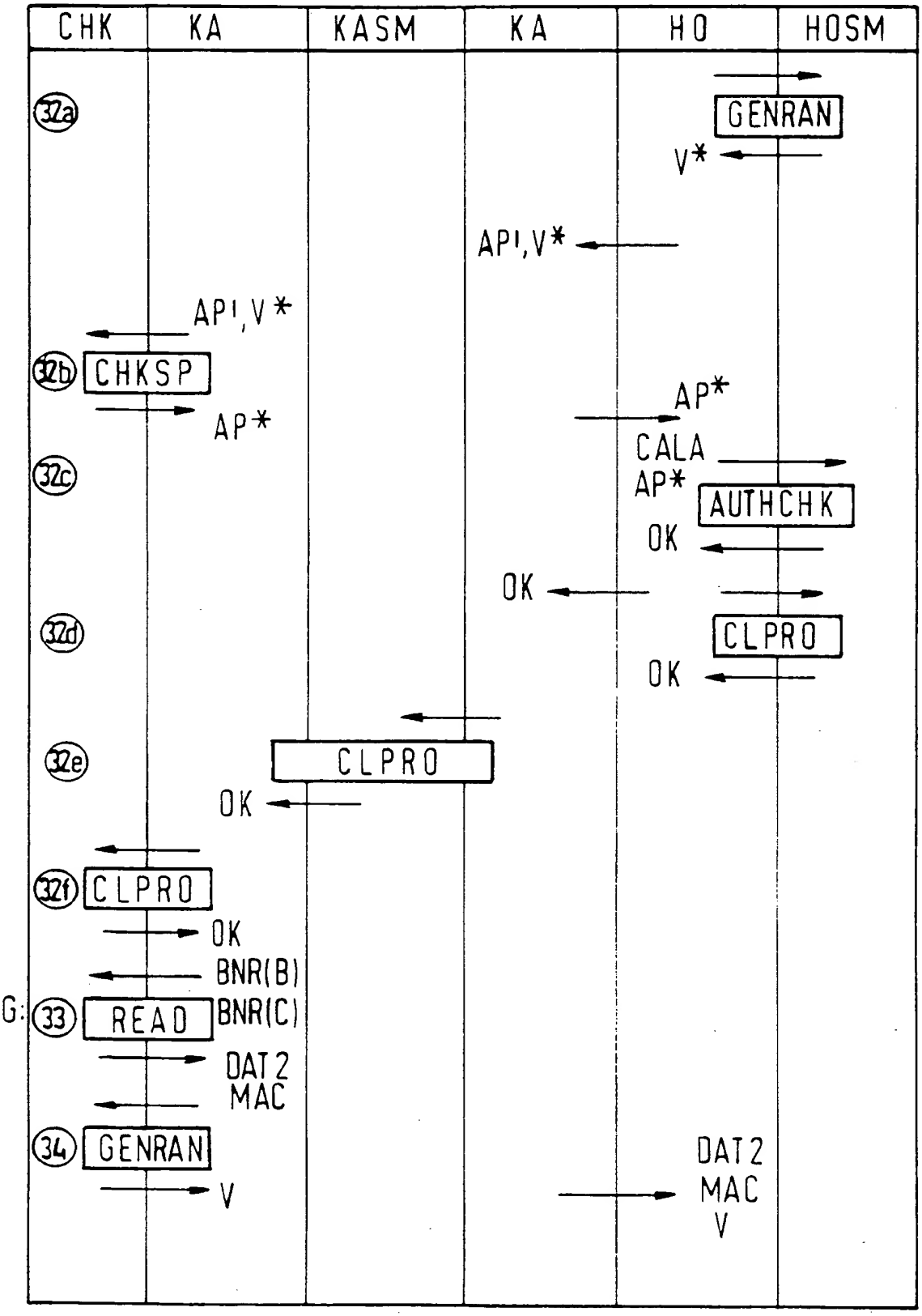
Nummer: DE 41 19 924 A1
Int. Cl.[5]: G 06 F 15/30
Offenlegungstag: 24. Dezember 1992

FIG 4d



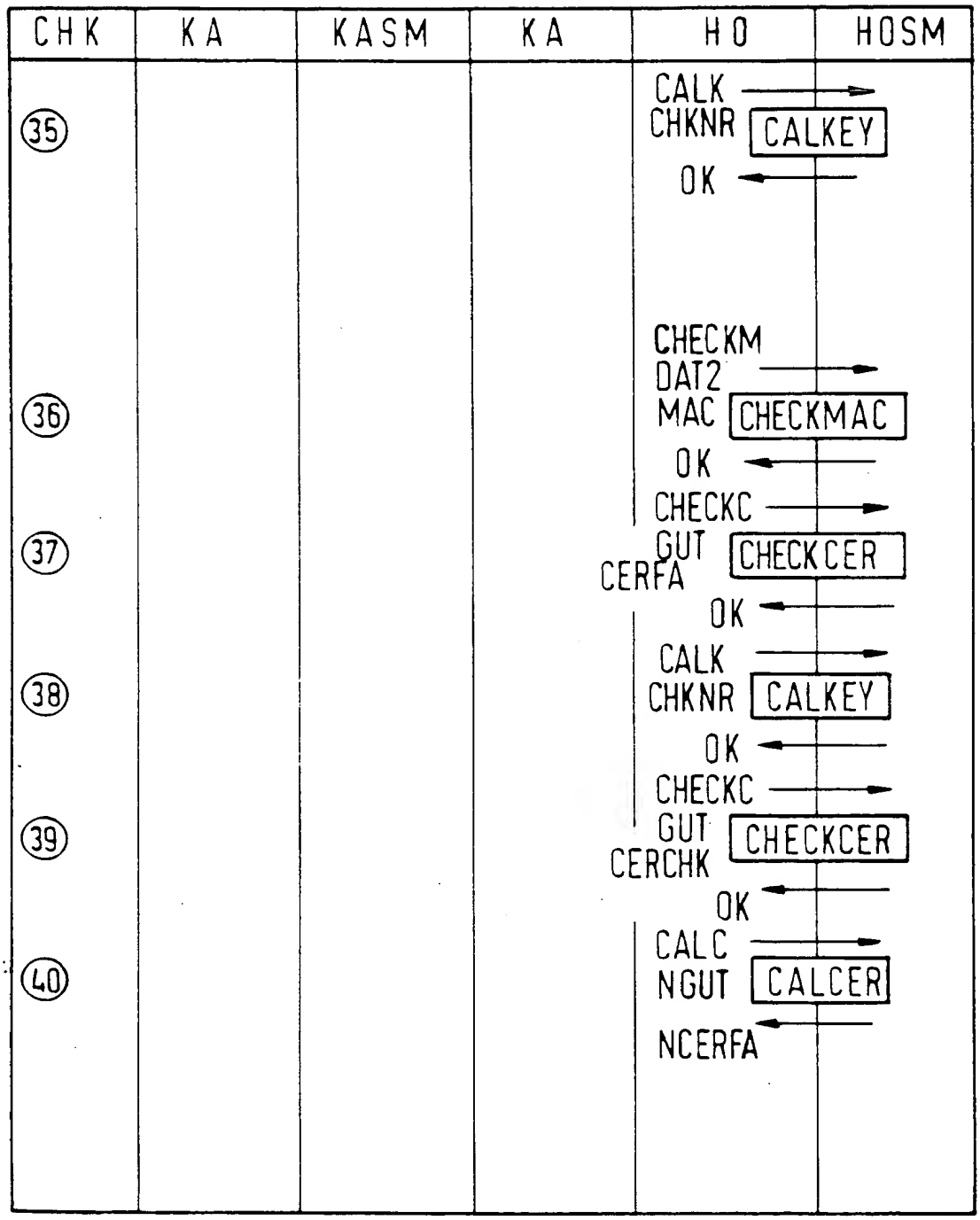
Nummer: DE 41 19 924 A1
Int. Cl.[5]: G 06 F 15/30
Offenlegungstag: 24. Dezember 1992

FIG 4e



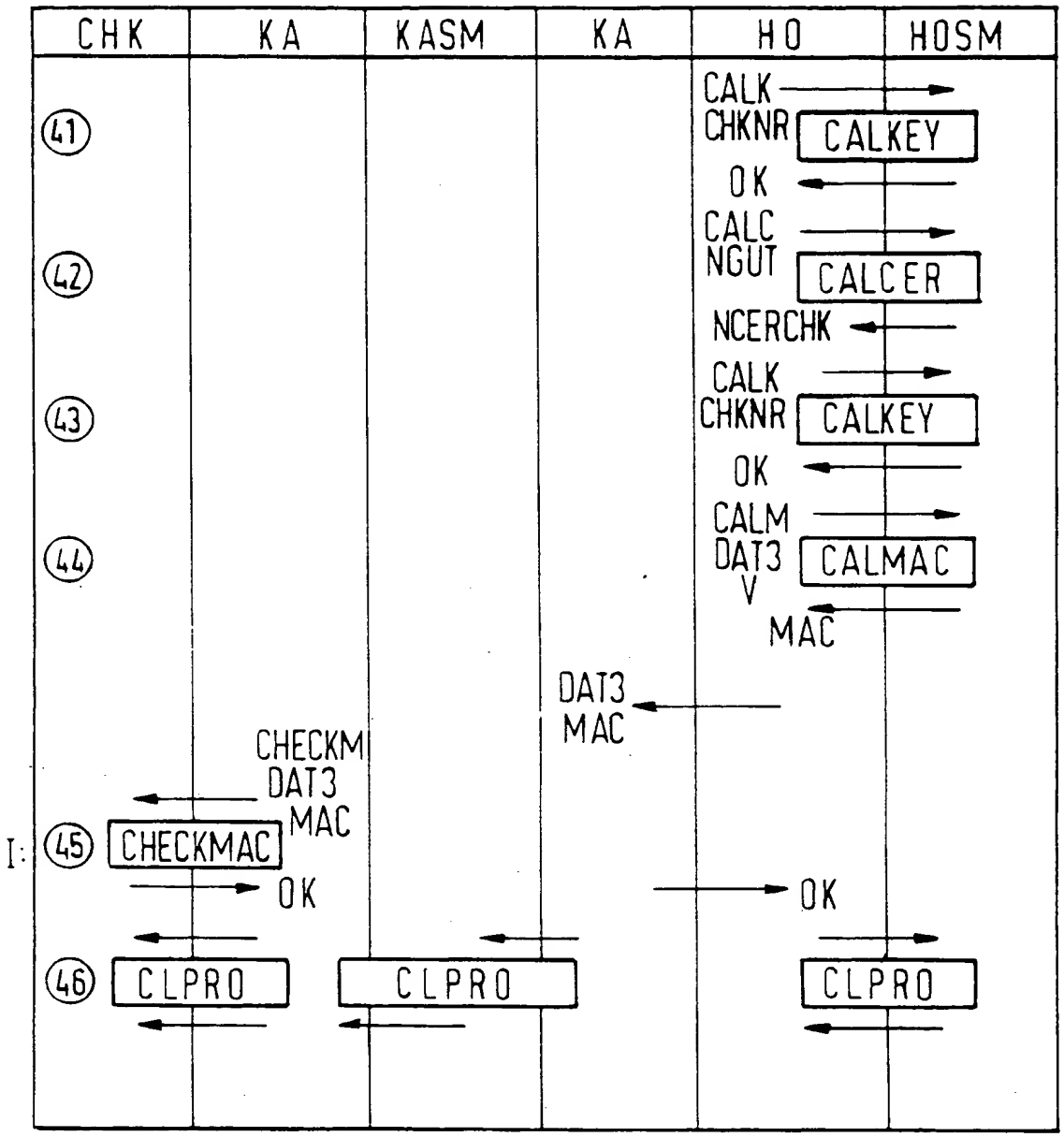
Nummer: DE 41 19 924 A1
Int. Cl.[5]: G 06 F 15/30
Offenlegungstag: 24. Dezember 1992

FIG 4f



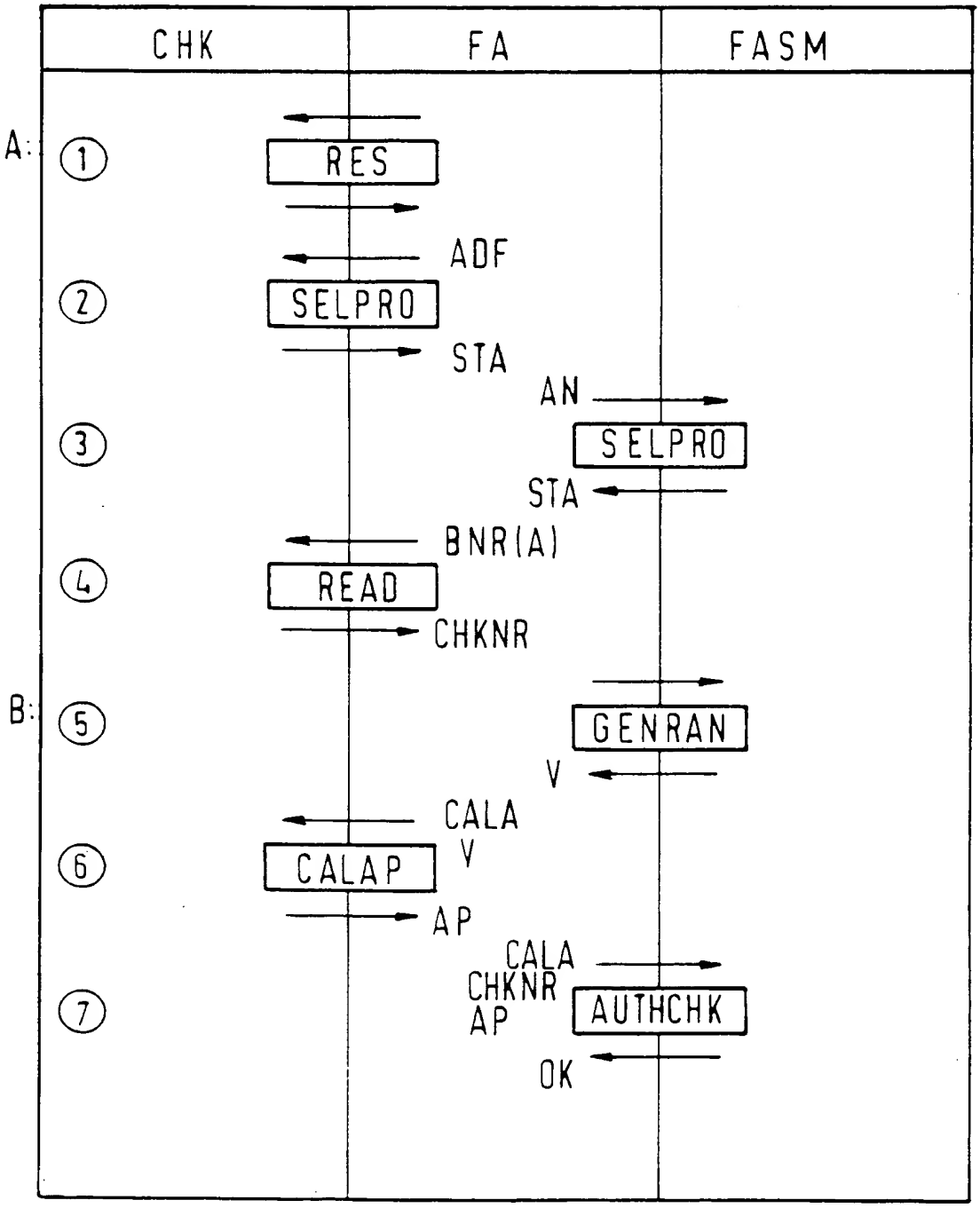
Nummer: DE 41 19 924 A1
Int. Cl.[5]: G 06 F 15/30
Offenlegungstag: 24. Dezember 1992

FIG 4g



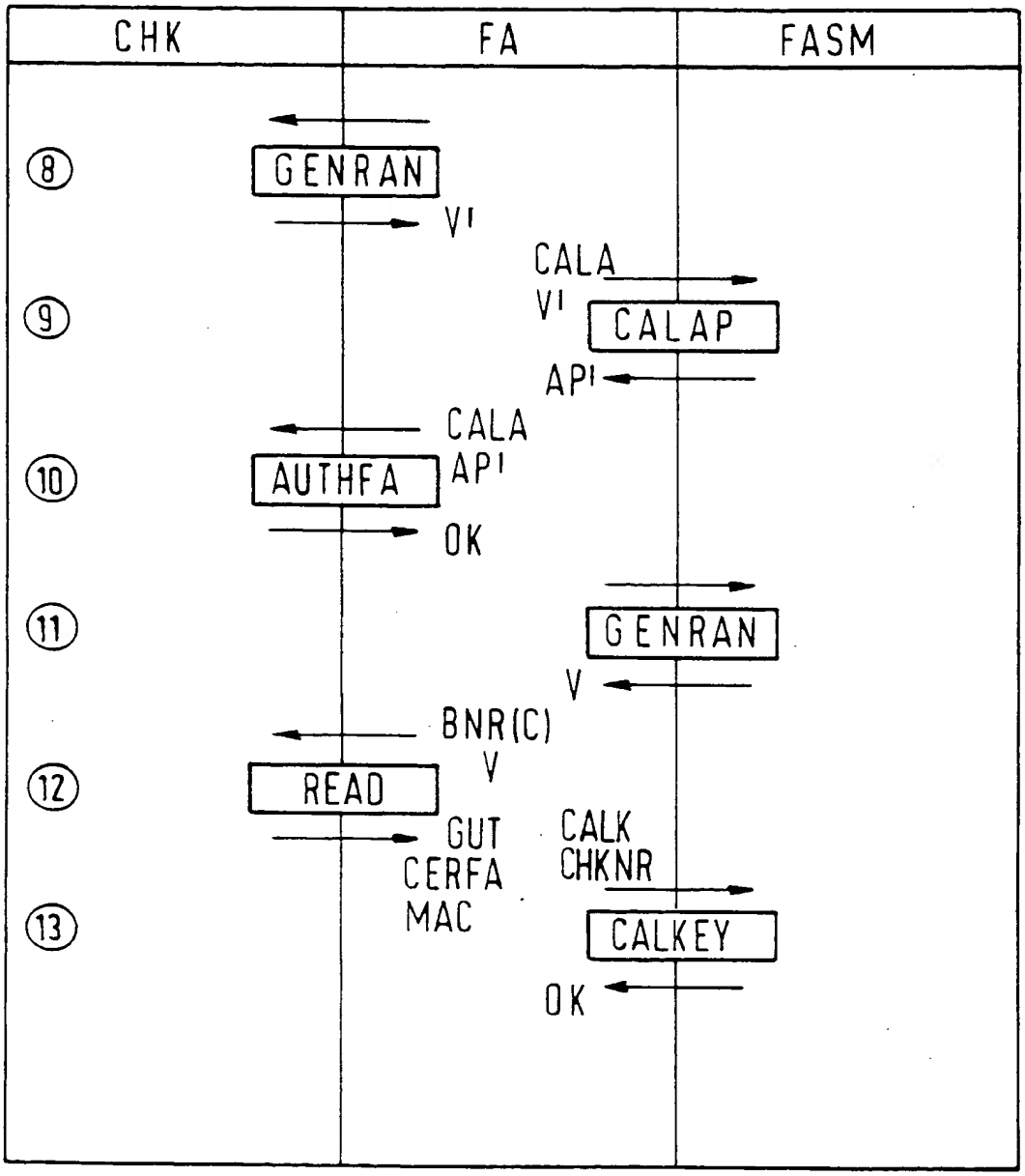
Nummer: DE 41 19 924 A1
Int. Cl.[5]: G 06 F 15/30
Offenlegungstag: 24. Dezember 1992

FIG 5a



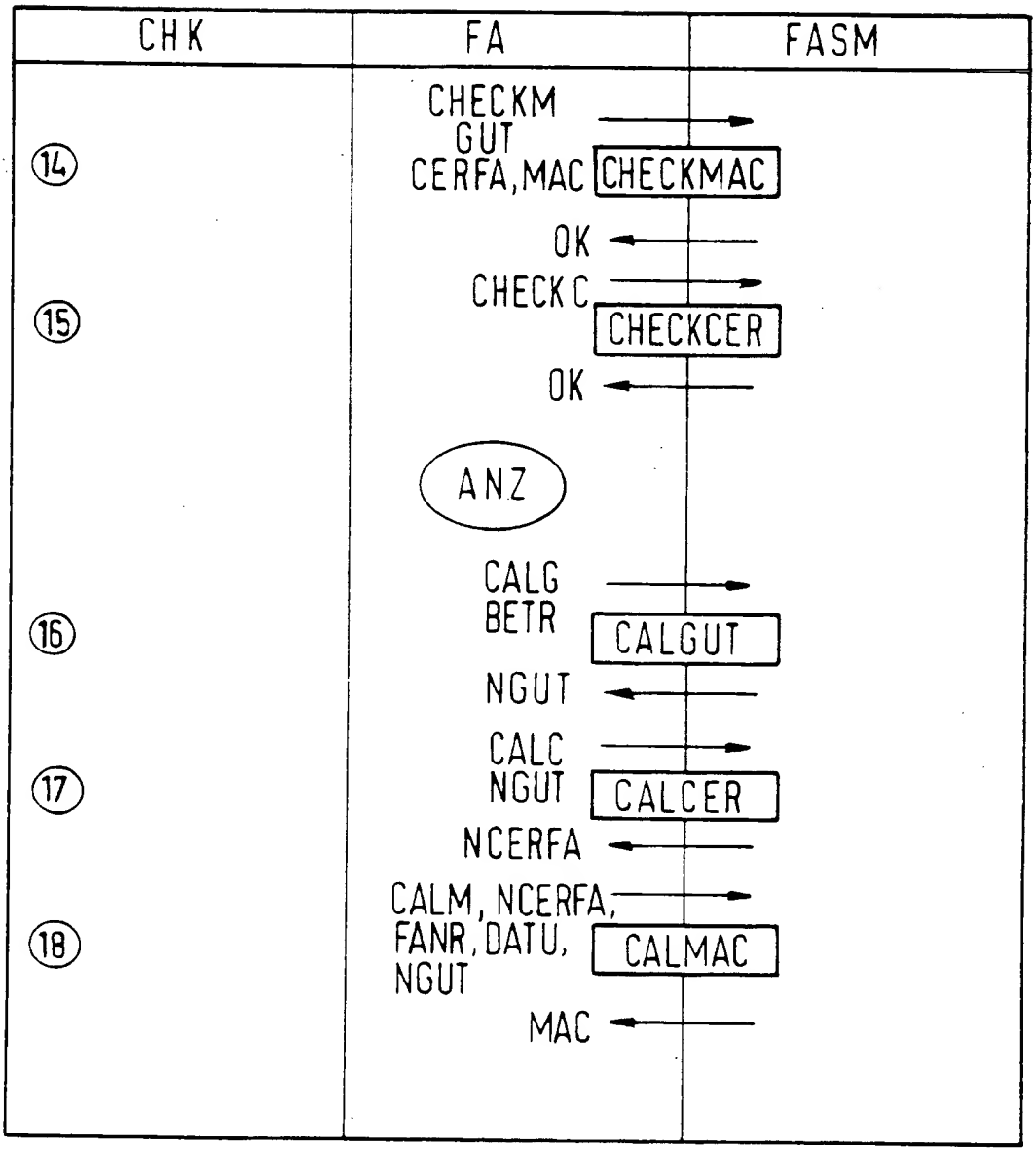
Nummer: DE 41 19 924 A1
Int. Cl.[5]: G 06 F 15/30
Offenlegungstag: 24. Dezember 1992

FIG 5b



Nummer: DE 41 19 924 A1
Int. Cl.[5]: G 06 F 15/30
Offenlegungstag: 24. Dezember 1992

FIG 5c



Nummer: DE 41 19 924 A1
Int. Cl.[5]: G 06 F 15/30
Offenlegungstag: 24. Dezember 1992

FIG 5d